Удостоверяющий центр Министерства здравоохранения и социального развития Российской Федерации

Руководство пользователя

Содержание

1 Определения и термины 3
2 Начало работы 9
3 Регистрация нового пользователя 11
4 Работа пользователя с маркером временного доступа 13
5 Работа зарегистрированного пользователя 18
5.1. Получение сертификата и списка отзыва УЦ 19
5.2. Формирование запроса на новый сертификат 19
Приложение 1 21
Приложение 2 23
Приложение 3 25

1 Определения и термины

Автоматизированная Система (АС)

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор безопасности

Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Безопасность информации

Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Документ в электронной форме (электронный документ)

Документ, в котором информация представлена в электронно-цифровой форме. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Доступ к информации (Доступ)

Ознакомление с информацией, ее обработка, в частности, копирование и модификация.

Закрытый ключ

Криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной цифровой подписи и/или шифрования данных.

Запрос на регистрацию

Сообщение, содержащее необходимую информацию для предварительной регистрации в качестве временного пользователя на Центре Регистрации. Формируется в Web-приложении самостоятельной регистрации, после чего передается через Центр Регистрации, где и обрабатывается. Результатом обработки является сообщение по электронной почте о порядке дальнейших действий.

Запрос на сертификат

Сообщение, содержащее необходимую информацию для получения сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр Регистрации Центру Сертификации, где и обрабатывается. Результатом обработки является выпущенный сертификат или сообщение об ошибке.

Запрос на отзыв сертификата

Сообщение, содержащее необходимую информацию для отзыва сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр Регистрации Центру Сертификации, где и обрабатывается. Результатом обработки является отзыв сертификата или сообщение об ошибке.

Защита от несанкционированного доступа (Защита от НСД)

Предотвращение или существенное затруднение несанкционированного доступа.

Защищенное средство вычислительной техники (защищенная АС)

Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

Идентификатор доступа

Уникальный признак субъекта или объекта доступа.

Идентификация

Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационное обеспечение (ИО)

Совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании.

Класс защищенности средств вычислительной техники, автоматизированной системы

Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Ключевая пара

Открытый и закрытый ключи.

Ключевой носитель

Объект системы, который может содержать один или несколько ключевых контейнеров. Каждый ключевой контейнер содержит следующую информацию: только ключ подписи, только ключ шифрования, ключ подписи и ключ шифрования одновременно. Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей и их целостности. Каждый контейнер является полностью самостоятельным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми ключами.

Комплекс средств защиты (КСЗ)

Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Компрометация ключа

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

1. Потеря ключевых носителей;
2. Потеря ключевых носителей с их последующим обнаружением;
3. Увольнение сотрудников, имевших доступ к ключевой информации;
4. Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
6. Нарушение печати на сейфе с ключевыми носителями;

7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

Различают два вида компрометации секретного ключа: **явную** и **неявную**. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

Многоуровневая защита

Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Модель защиты

Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

Модуль автоматизированной системы (модуль АС)

Часть АС, реализующая одну или более взаимосвязанных функций АС.

Нарушитель правил разграничения доступа (Нарушитель ПРД)

Субъект доступа, осуществляющий несанкционированный доступ к информации.

Несанкционированный доступ к информации (НСД)

Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Объект доступа

Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Открытый ключ

Криптографический ключ, который связан с закрытым ключом с помощью особого математического соотношения. Открытый ключ известен другим пользователям системы и предназначен для проверки электронной цифровой подписи и шифрования. При этом открытый ключ не позволяет вычислить закрытый ключ.

Плановая смена ключей

Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Подтверждение подлинности ЭЦП

Положительный результат проверки правильности ЭЦП, выработанной правомочным лицом из исходной информации путем применения принадлежащего ему закрытого ключа ЭЦП, полученный с использованием зарегистрированного и сертифицированного открытого ключа ЭЦП.

Показатель защищенности средств вычислительной техники (Показатель защищенности)

Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

Пользователь автоматизированной системы (пользователь АС)

Лицо, участвующее в функционировании АС или использующее результаты ее функционирования.

Пользователь АС зарегистрированный

Пользователь АС или системный сервис, имеющий учетную запись в АС.

Правила разграничения доступа (ПРД)

Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Проверка электронной подписи документа

Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним - недействительной.

Программное обеспечение (ПО)

Совокупность программ на носителях информации и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС.

Санкционированный доступ к информации (СД)

Доступ к информации, не нарушающий правила разграничения доступа.

Сертификат

1. Документ, выданный и заверенный удостоверяющим центром, подтверждающий принадлежность открытого ключа ЭЦП определенному лицу. Сертификат может содержать дополнительную информацию, необходимую для обеспечения безопасности использования открытого ключа ЭЦП. В случае, когда сертификат выдается в форме электронного документа, он подписывается ЭЦП этого центра.
2. Электронный документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью его издателя. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует.

Формат сертификата определен в рекомендациях ITU-T 1997 года X.509 и рекомендациях IETF 1999 года RFC 2459.

Сертификат защиты

Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

Сертификация уровня защиты

Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите.

Система защиты информации от несанкционированного доступа (СЗИ НСД)

Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Система защиты секретной информации (СЗСИ)

Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.

Система разграничения доступа (СРД)

Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Список отзыва

Список отозванных сертификатов (CRL – Certificate Revocation List). УЦ поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов. Пользователи УЦ могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

Средство защиты от несанкционированного доступа (Средство защиты от НСД)

Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Средство криптографической защиты информации (СКЗИ)

Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Средство электронной цифровой подписи

Совокупность программных и технических средств, реализующих функцию выработки и проверки электронной цифровой подписи.

Субъект доступа

Лицо или системный сервис (процесс), действия которого регламентируются правилами разграничения доступа.

Техническое обеспечение (ТО)

Совокупность средств реализации управляющих воздействий, средств получения, ввода, подготовки, преобразования, обработки, хранения, регистрации, вывода, отображения, использования и передачи данных с конструкторской и эксплуатационной документацией.

Уровень полномочий субъекта доступа

Совокупность прав доступа субъекта доступа.

Учетная запись

Информация, хранимая в АС, служащая для идентификации, аутентификации, авторизации действий пользователей АС и системных сервисов (логин, пароль, цифровой сертификат), а также содержащая прочие, необходимые для функционирования АС характеристики пользователей и сервисов (E-mail, адрес и т.п.).

Функция автоматизированной системы (функция АС)

Совокупность действий АС, направленная на достижение определенной цели, на выполнение определенного технологического процесса.

Центр по удостоверению подлинности электронной цифровой подписи (удостоверяющий центр)

Юридическое лицо или выделенное подразделение юридического лица, обладающие правомочиями на удостоверение принадлежности конкретного открытого ключа ЭЦП определенному пользователю.

Целостность информации

Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Центр Сертификации (Удостоверяющий центр)

Компонент Удостоверяющего центра. Выполняет функции службы сертификации: выпуск сертификатов, отзыв сертификатов, а также генерацию списков отзыва.

Центр Регистрации

Компонент Удостоверяющего центра. Выполняет функции промежуточного звена, осуществляющего передачу запросов от пользователей и администраторов Центра Регистрации центру сертификации. В процессе этой передачи осуществляется аутентификация пользователя, проверка корректности передаваемой им информации, а также фиксация этой информации в базе данных ЦР.

Шифрование

Процесс зашифрования или расшифрования.

Шифрование информации – взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Если зашифрование и расшифрование осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае — асимметричным.

Прочитать зашифрованное сообщение (информацию) может только пользователь, имеющий тот же секретный ключ шифрования.

Электронная цифровая подпись (ЭЦП)

Последовательность символов, полученная в результате криптографического преобразования исходной информации с использованием закрытого ключа ЭЦП, которая позволяет подтверждать целостность и неизменность этой информации, а также ее авторство при условии использования открытого ключа ЭЦП и его сертификата.

2 Начало работы

Для работы с Удостоверяющим центром необходимо следующее программное обеспечение:

- Операционная система Microsoft Windows 2000 и выше;
- Интернет-браузер Microsoft Internet Explorer версии 7.0 и выше;
- Сертифицированное средство криптографической защиты КриптоПро CSP версии 3.6 и выше;
- Обновления безопасности MS Windows (для версии Windows XP): Q323172 и Q328145;
- Компонент CAPICOM версии 2.1.0.1 (http://www.microsoft.com/downloads/ru-ru/details.aspx?FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6&displayLang=ru).

Удостоверяющий центр (далее – УЦ) находится по адресу https://crt.rosminzdrav.ru



Этот адрес необходимо добавить в «Надежные узлы». Для этого требуется внутри браузера *Internet Explorer* открыть «**Свойства обозревателя**», перейти на вкладку «**Безопасность**», пометить мышью пиктограмму «**Надежные узлы**» и нажать появившуюся кнопку «**Узлы**». В отобразившемся окне ввести адрес УЦ и нажать кнопку «**Добавить**». После этого браузер необходимо перезапустить.

Для проведения работ с сертификатами необходимо воспользоваться ссылкой «**Вход для пользователей удостоверяющего центра**» или ввести в адресной строке следующий адрес: https://crt.rosminzdrav.ru/ui/. При переходе по данному адресу отобразится страница, изображённая на рисунке 1. Данная страница доступна только при установленном криптопровайдере.

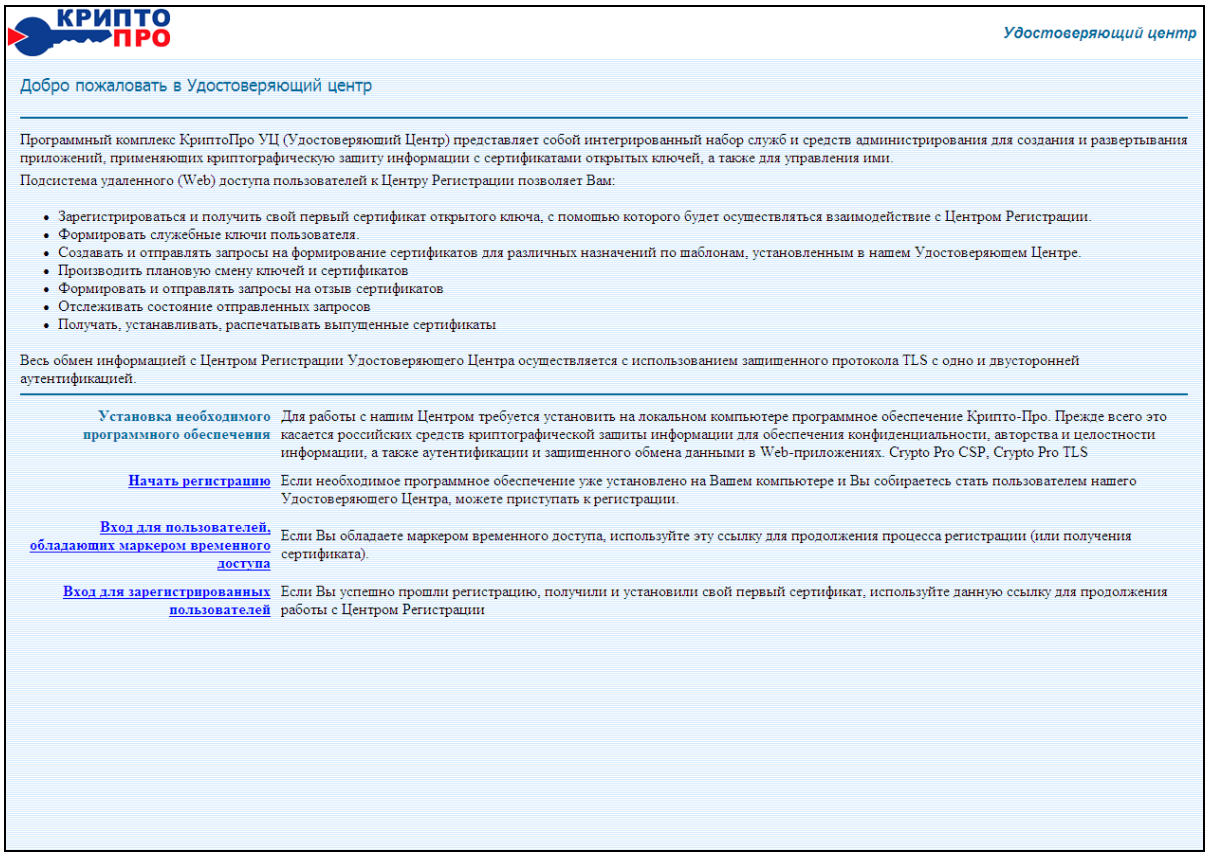


Рисунок 1 – Начальная страница УЦ

3 Регистрация нового пользователя

Внимание! *Если у пользователя имеется личный сертификат, выпущенный УЦ Минздравсоцразвития, это значит, что он уже зарегистрирован в Удостоверяющем центре и может пропустить этот раздел.*

При первом посещении УЦ необходимо пройти процедуру регистрации нового пользователя. Для этого на главной странице необходимо нажать на ссылку «**Начать регистрацию**» или перейти вручную по адресу https://crt.rosminzdrav.ru/ui/Register/RegGetSubject.asp. Отобразится раздел «**Страница самостоятельной регистрации**» (рисунок 2).

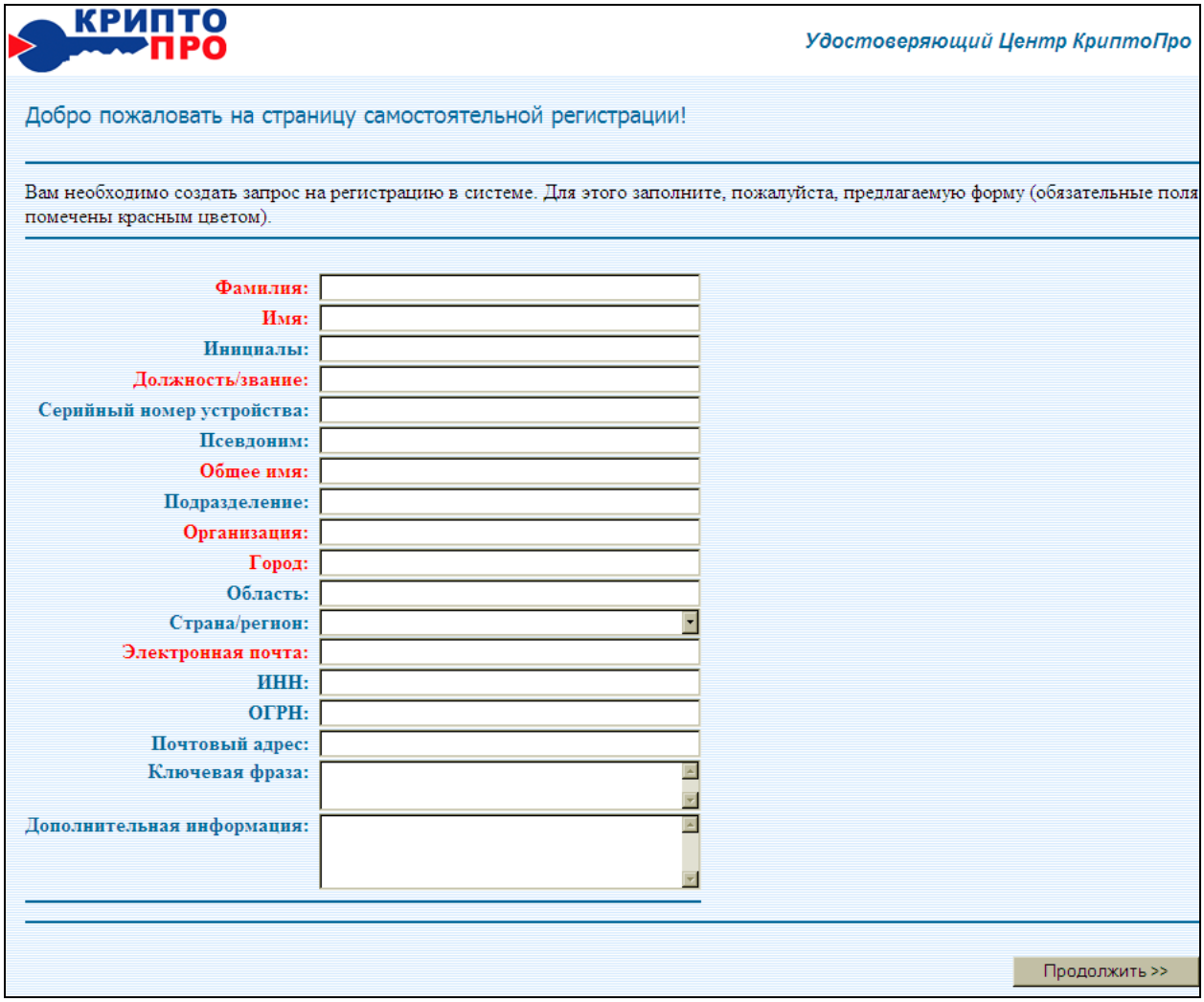


Рисунок 2 – Страница самостоятельной регистрации

В предложенной форме требуется заполнить все известные поля. Минимальный набор обязательных полей выделен красным цветом. Ввод данных необходимо осуществлять внимательно, они должны соответствовать информации, направленной в адрес Министерства официальным письмом. На поле «**Общее имя**» распространяются особенные правила заполнения, которые описаны в Приложении 1. Адрес, указанный поле «**Электронная почта**», будет использован для автоматического информирования о состоянии заявок. Для упрощения идентификации пользователя также рекомендуется заполнить поля «**Инициалы**» и «**Область**». Поле Страна/регион заполняется из выпадающего списка выбором значения «**RU**».

После заполнения и проверки формы, её следует отправить нажатием на кнопку «**Продолжить >>**». На открывшейся странице будет предложено сохранить персональный маркер временного доступа (рисунок 3).

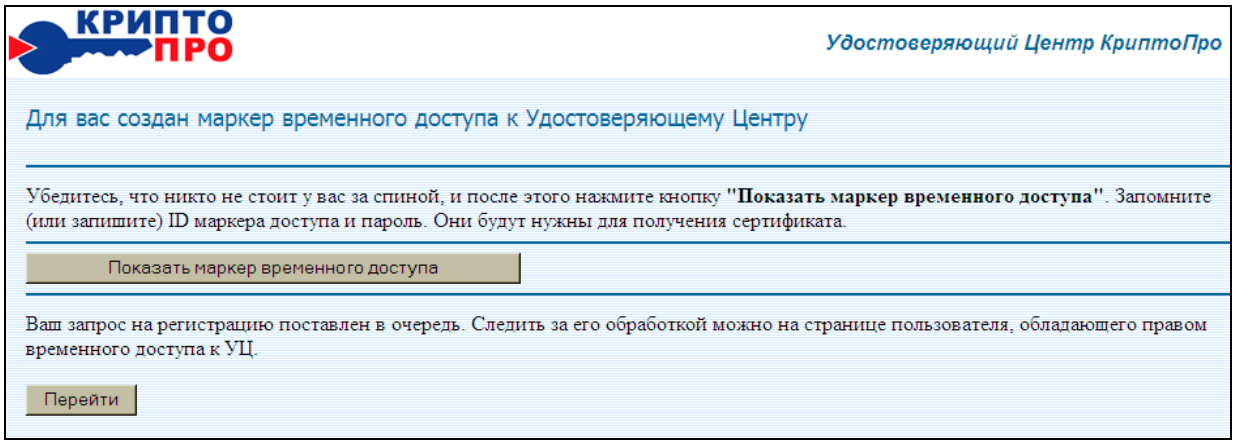


Рисунок 3 – Маркер временного доступа

Необходимо нажать на кнопку «**Показать маркер временного доступа**», после чего запомнить или записать ID маркера и пароль. Эти данные необходимы пользователю для того, чтобы авторизоваться в УЦ и следить за ходом рассмотрения заявки на регистрацию. Заявки на регистрацию рассматриваются в течение трёх дней с момент получения официального письма.

Для того чтобы перейти в раздел для пользователей, обладающих маркером временного доступа, необходимо нажать на кнопку «**Перейти**». Отобразится «**Страница пользователя, обладающего правом временного доступа к УЦ**» (рисунок 5).

4 Работа пользователя с маркером временного доступа

После создания запроса на регистрацию и получения маркера временного доступа пользователь получает возможность авторизоваться в УЦ и следить за ходом рассмотрения заявки. Для этого, находясь на начальной странице УЦ (рисунок 1), необходимо нажать на ссылку «**Вход для пользователей, обладающих маркером временного доступа**», либо вручную перейти по адресу https://crt.rosminzdrav.ru/ui/Register/RegTemporaryUser.asp. Отобразится форма авторизации пользователя с маркером временного доступа (рисунок 4).

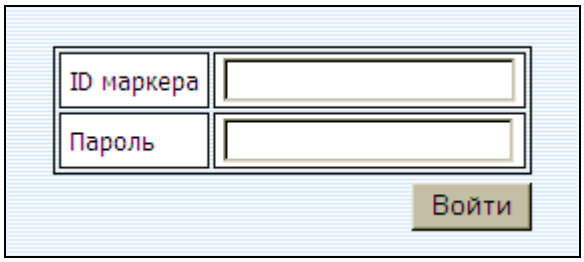


Рисунок 4 – Авторизация пользователя с маркером временного доступа

При удачной авторизации отобразится «**Страница пользователя, обладающего правом временного доступа к УЦ**» (рисунок 5).

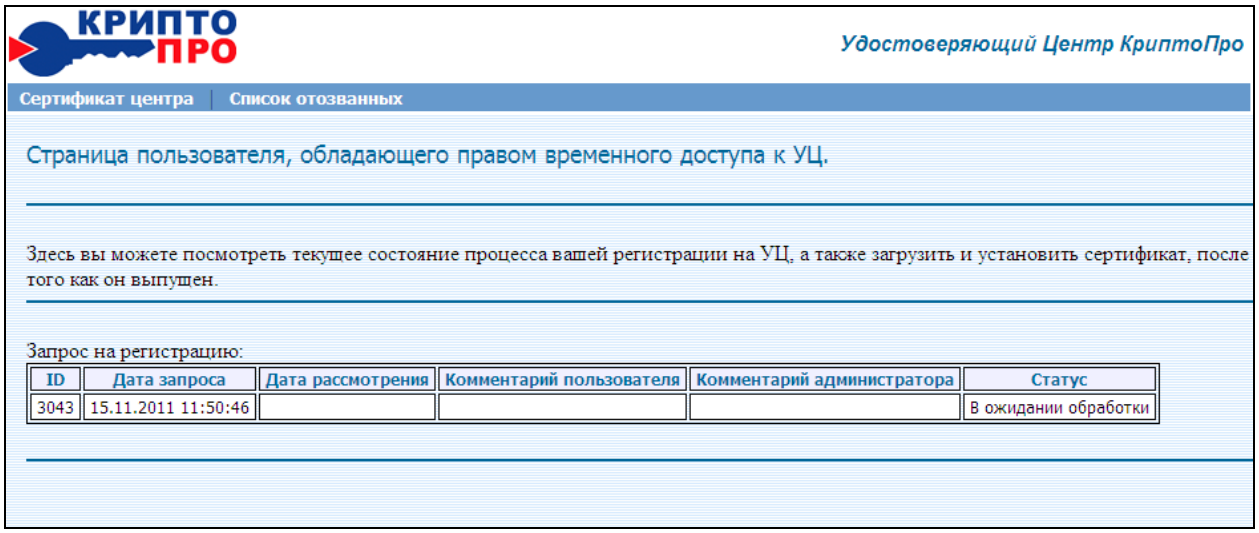


Рисунок 5 – Страница пользователя, обладающего правом временного доступа к УЦ

По завершению обработки запроса на регистрацию (об этом пользователю будет направлено уведомление на адрес электронной почты) на странице отобразится кнопка для создания первого рабочего сертификата (рисунок 6).

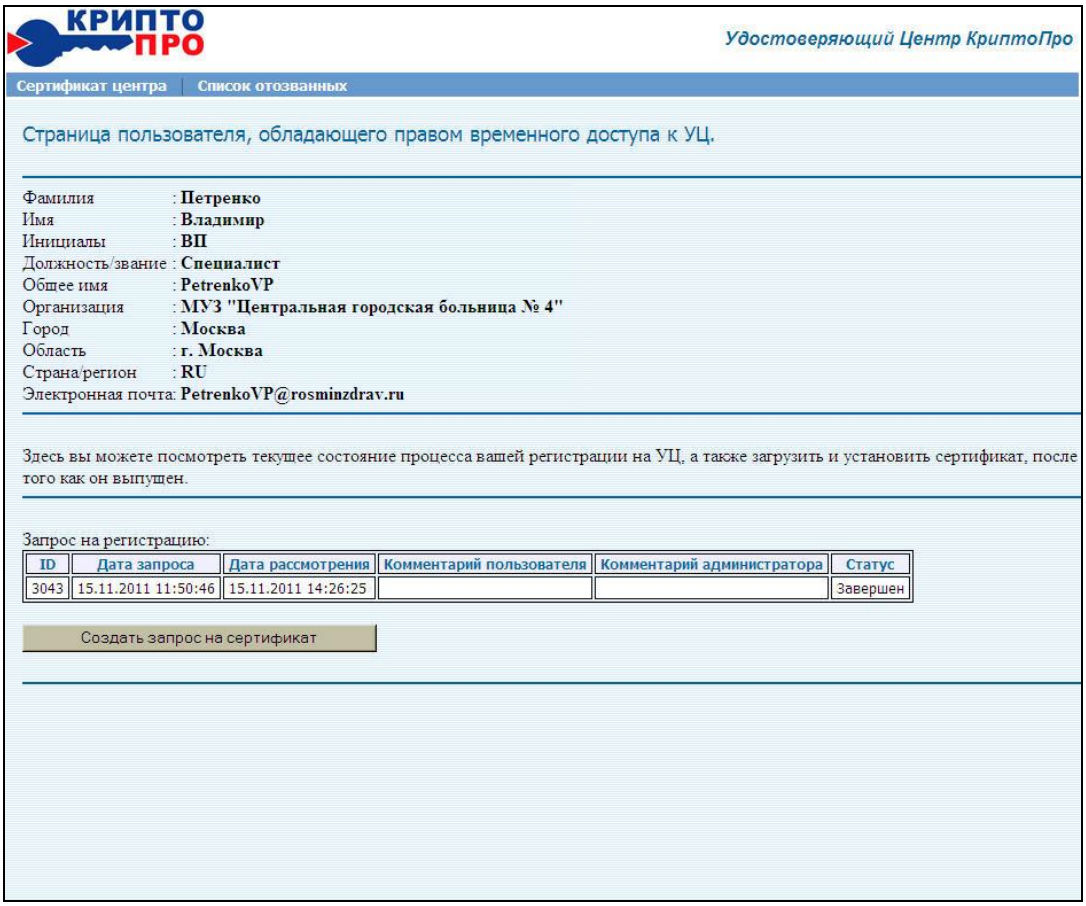


Рисунок 6 – Страница пользователя, обладающего правом временного доступа к УЦ

Для создания запроса на сертификат, необходимо нажать на кнопку «**Создать запрос на сертификат**». Отобразится страница «**Запрос на сертификат зарегистрированного пользователя**» (рисунок 7). В предложенной форме необходимо заполнить поле «**Шаблон сертификата**», указав там «**Сертификат пользователя УЦ**». Дополнительно можно оставить короткий комментарий для администратора УЦ в поле «**Информация**».

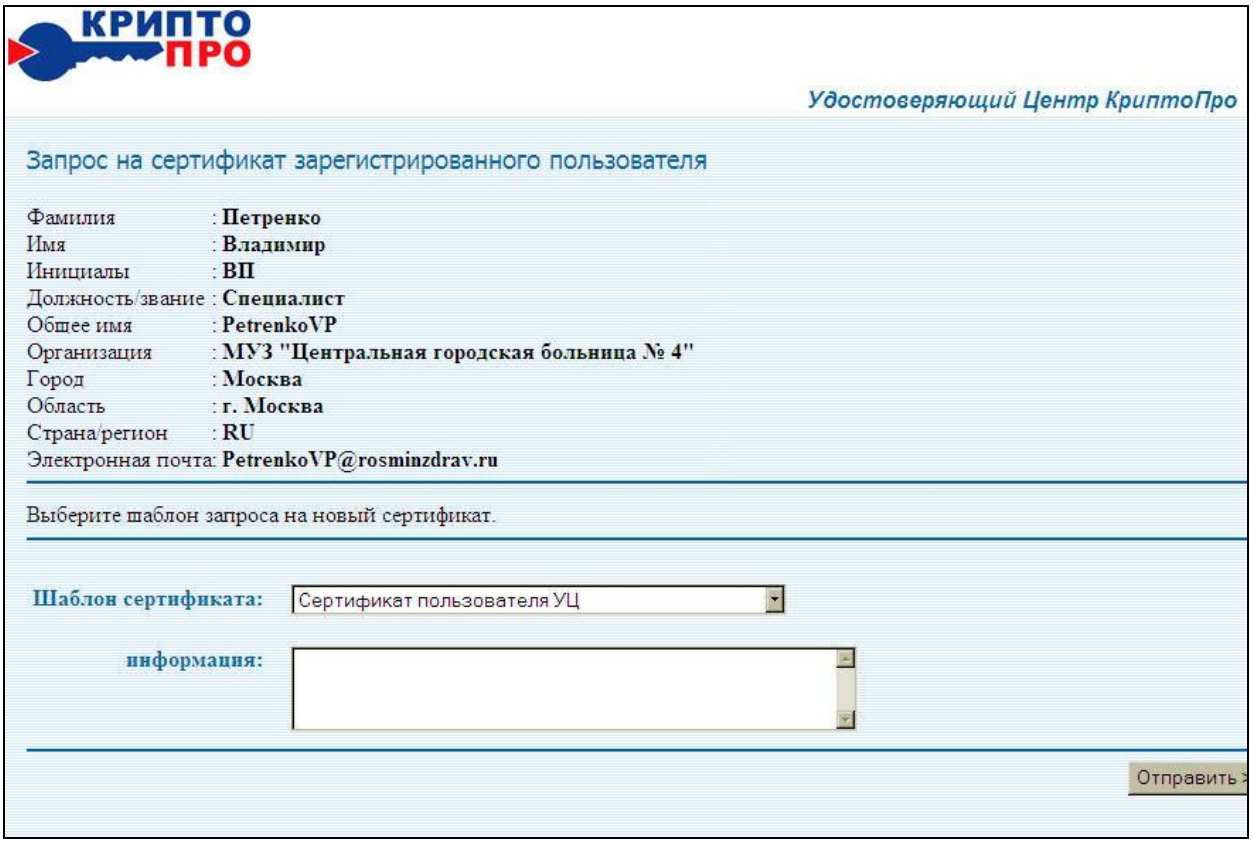


Рисунок 7 – Запрос на сертификат зарегистрированного пользователя

Для продолжения требуется подготовить отформатированный носитель (Rutoken, eToken или др.; в Приложении 2 приведены руководства для некоторых типов устройств). Носитель должен быть вставлен в компьютер или смонтирован и готов к записи на него сертификата. Далее следует нажать кнопку «**Отправить**». Начнётся процесс генерации запроса на сертификат. Возможно появления предупреждения «**Потенциальная ошибка сценария**» (рисунок 8), в нём следует нажать кнопку «**Да**».

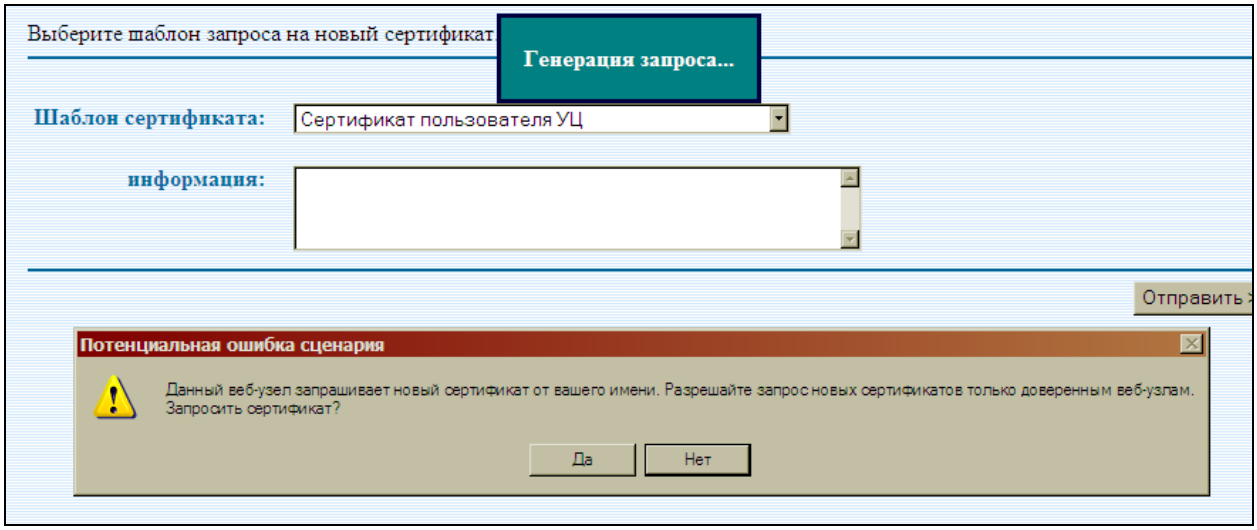


Рисунок 8 – Предупреждение безопасности

Далее требуется выбрать подготовленный носитель в общем списке доступных носителей (рисунок 9) и, следуя подсказкам на экране, сгенерировать ключ, который будет записан на устройство, и завершить формирование запроса.

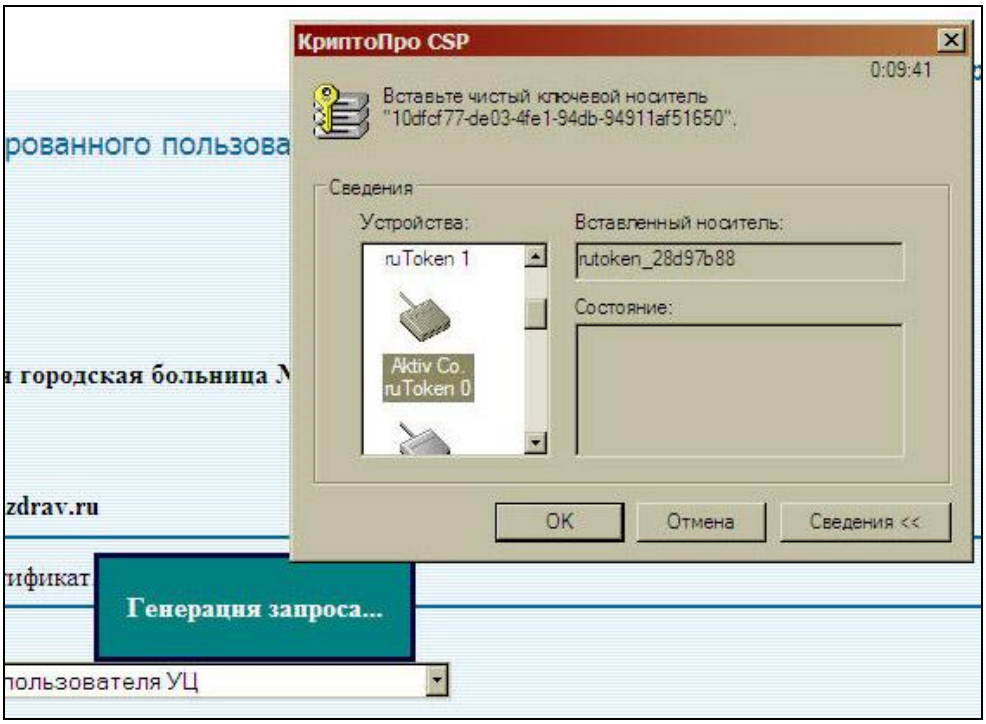


Рисунок 9 – Выбор носителя

Запрос будет автоматически отправлен на сервер. В случае успешного ответа, появится сообщение о том, что запрос поставлен в очередь (рисунок 10).

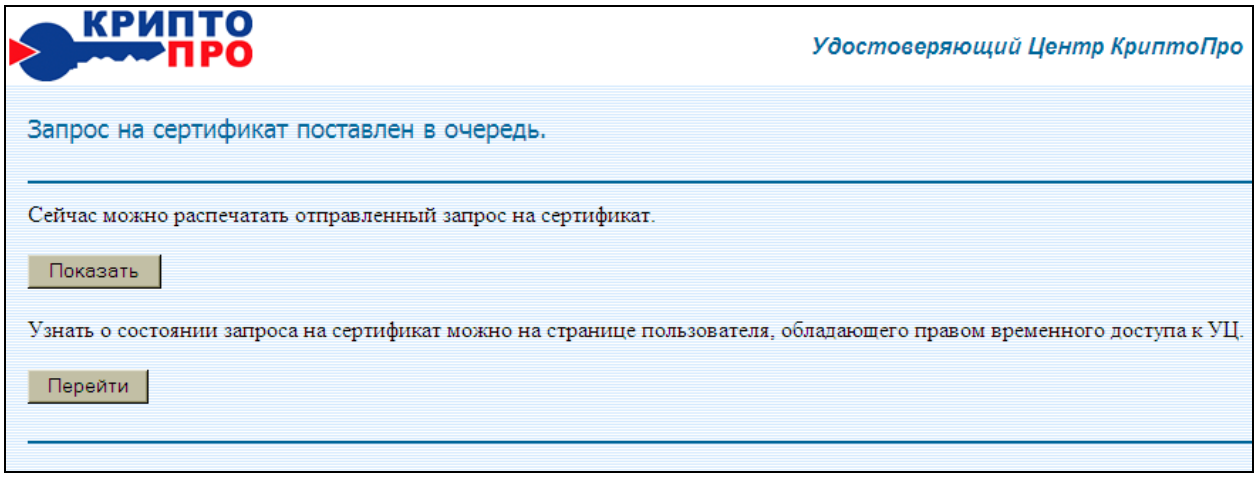


Рисунок 10 – Страница успешной отправки запроса

Вместе с этим сообщением будет предложено получить и распечатать бумажную копию запроса, а также вернуться на страницу пользователя, обладающего маркером доступа. Страница пользователя будет отображать ход рассмотрения запроса на сертификат (рисунок 11). В процессе рассмотрения сертификата на странице также будет доступна кнопка «**Показать**», позволяющая получить и распечатать бумажную копию запроса.

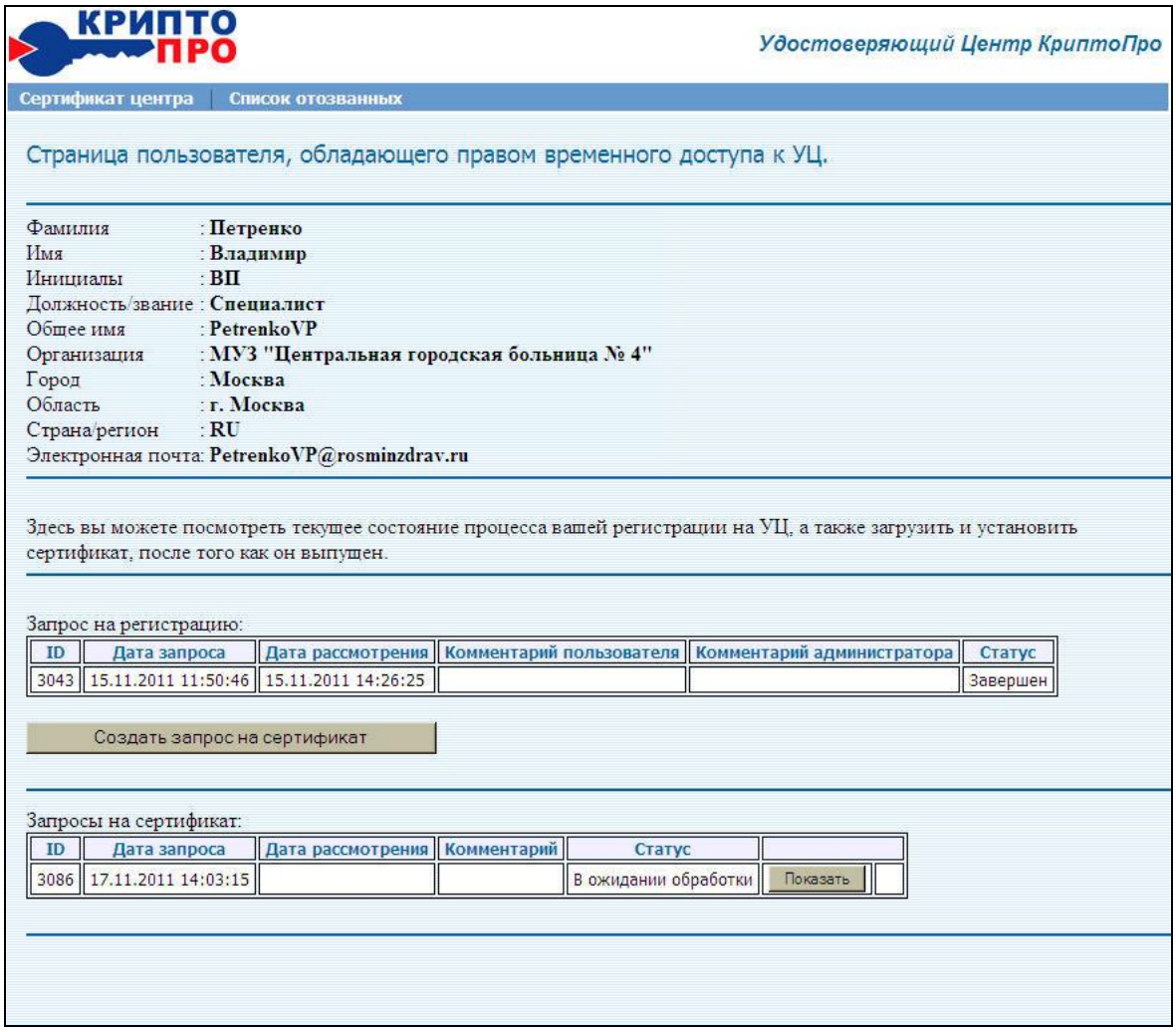


Рисунок 11 – Страница пользователя с отправленным запросом на сертификат

По завершению обработки запроса на сертификат (об этом пользователю будет направлено уведомление на адрес электронной почты) на странице отобразится кнопка для получения первого рабочего сертификата. Для продолжения носитель, на который был записан ключ, вновь должен быть вставлен в компьютер или смонтирован. Далее следует нажать кнопку «**Получить сертификат**» и, следуя инструкциям на экране, установить готовый сертификат на носитель, а также в хранилище сертификатов «**Личные**».

После этого с помощью полученного сертификата можно авторизоваться в требуемой информационной системе. Подробности использования персонального ключа доступа для работы в информационной системе описаны в соответствующем руководстве. Также с помощью этого сертификата впредь можно авторизоваться и в самом УЦ.

Внимание! *Доступ к информационной системе настраивается в течение 24 часов с момента изготовления сертификата.*

5 Работа зарегистрированного пользователя

После получения первого рабочего сертификата, пользователь считается зарегистрированным и может использовать данный сертификат, как и все последующие, для авторизации в УЦ.

Чтобы перейти в раздел для зарегистрированного пользователя необходимо, находясь на начальной странице УЦ (рисунок 1), нажать на ссылку «**Вход для зарегистрированных пользователей**», либо вручную перейти по адресу https://crt.rosminzdrav.ru/ui/user/user.asp. После этого будет предложен выбор личного сертификата для авторизации в УЦ. Далее отобразится страница зарегистрированного пользователя (рисунок 12).

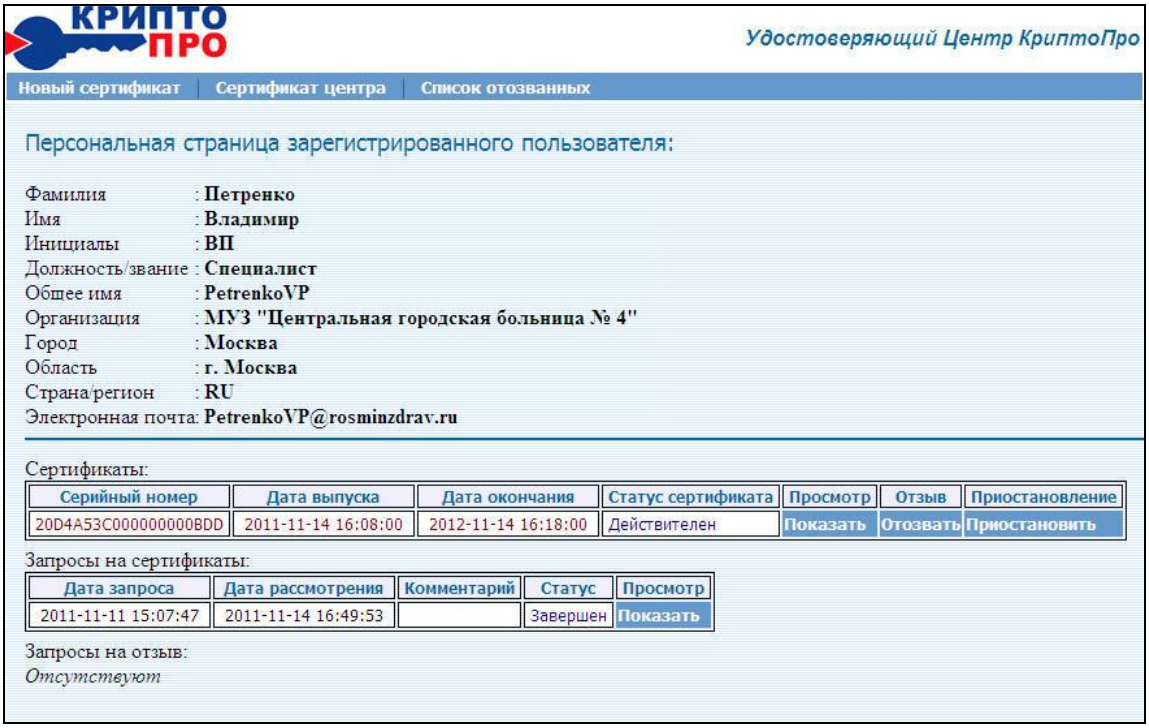


Рисунок 12 – Страница зарегистрированного пользователя

В этом разделе пользователь УЦ может:

- просмотреть список всех своих сертификатов, запросов на сертификат и запросов на отзыв сертификата;
- получить печатный бланк сертификата или запроса;
- сформировать запрос на отзыв любого из выпущенных сертификатов, либо на приостановление его действия на определённый срок;
- сформировать запрос на новый сертификат;
- получить сертификат и список отзыва УЦ.

Внимание! *Для формирования запросов на сертификат, на отзыв сертификата или на приостановление сертификата на компьютере пользователя должен быть установлен компонент CAPICOM, а УЦ добавлен в «Надёжные узлы». Подробнее в разделе 2.*

5.1. Получение сертификата и списка отзыва УЦ

Для получения сертификата или списка отозванных сертификатов УЦ необходимо нажать на соответствующую надпись в верхней части страницы. Предложенный файл необходимо сохранить в удобном месте, после чего открыть «Проводник» и перейти в папку с файлом. Далее требуется нажать правой кнопкой мыши на файл и выбрать пункт «**Установить …**».

5.2. Формирование запроса на новый сертификат

Для получения сертификата или списка отозванных сертификатов УЦ необходимо нажать на надпись «Новый сертификат» в верхней части страницы. Процесс создания запроса на сертификат протекает аналогично процессу создания первого рабочего сертификата, описанному в разделе 4. Важным отличием является необходимость в установленном компоненте CAPICOM. При открытии страницы будет также предложено дополнение для CAPICOM (рисунок 13), на него необходимо ответить утвердительно («*Установить*») и дождаться перезагрузки страницы.

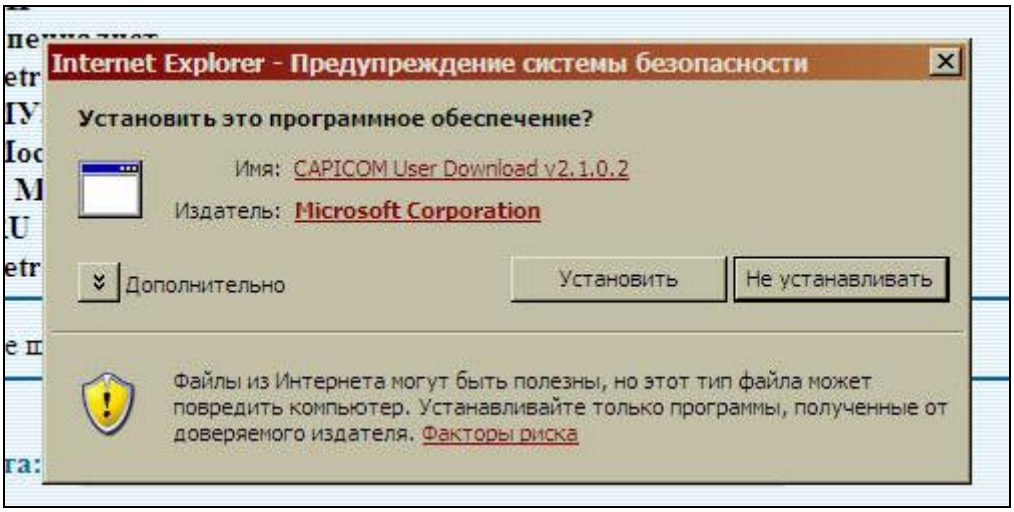


Рисунок 13 – Предупреждение об установке дополнения для CAPICOM

После нажатия на кнопку «**Отправить**» появятся два предупреждения (рисунок 14), на которые также требуется ответить утвердительно («*Yes*»).

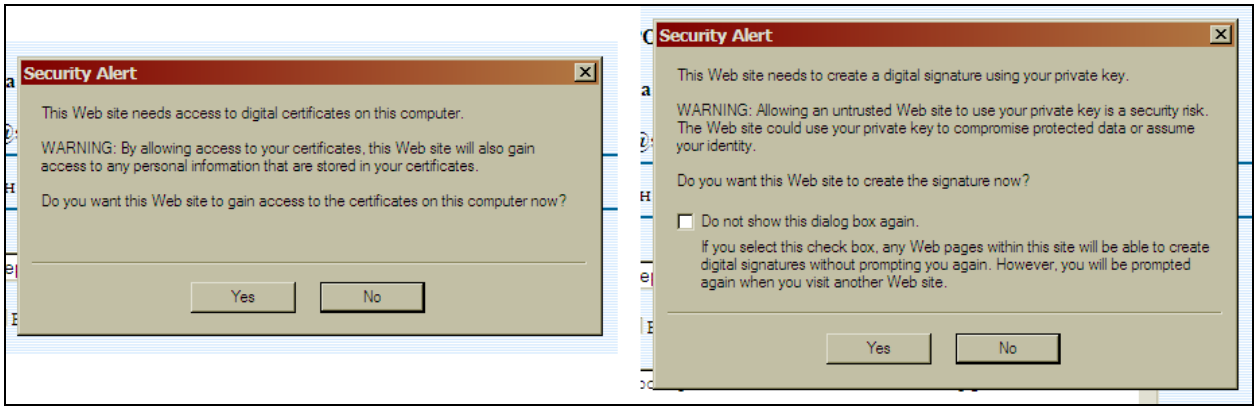


Рисунок 14 – Предупреждения безопасности

Далее сгенерированный ключ будет записан на носитель и запрос будет отправлен сервер. В результате отобразится страница зарегистрированного пользователя, на которой добавлена информация о созданном запросе (рисунок 15).

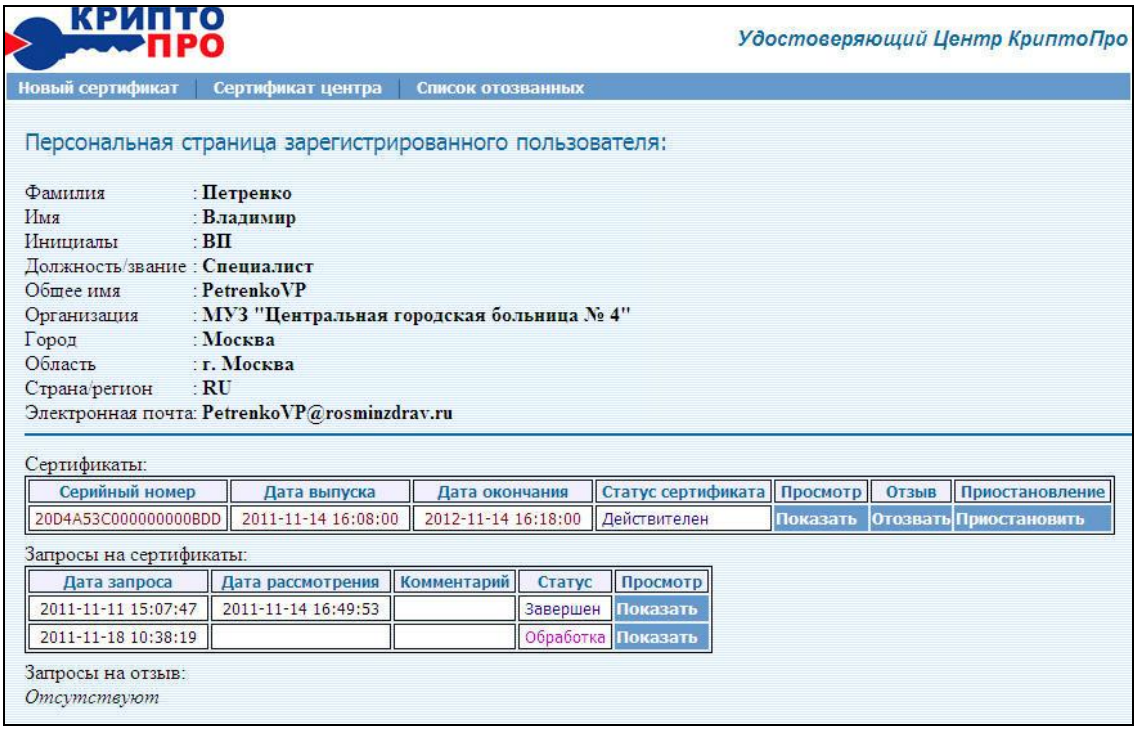


Рисунок 15 – Запрос создан и находится на обработке

По завершению обработки запроса на сертификат (об этом пользователю будет направлено уведомление на адрес электронной почты) на странице отобразится кнопка для получения и установки нового сертификата. Для продолжения носитель с ключом вновь должен быть вставлен в компьютер или смонтирован. Далее следует нажать кнопку «**Установить**» рядом с новым сертификатом и, следуя инструкциям на экране (рисунок 16), установить готовый сертификат на носитель, а также в хранилище сертификатов «**Личные**».

После установки сертификата обязательно необходимо подтвердить установку, нажав соответствующую кнопку.

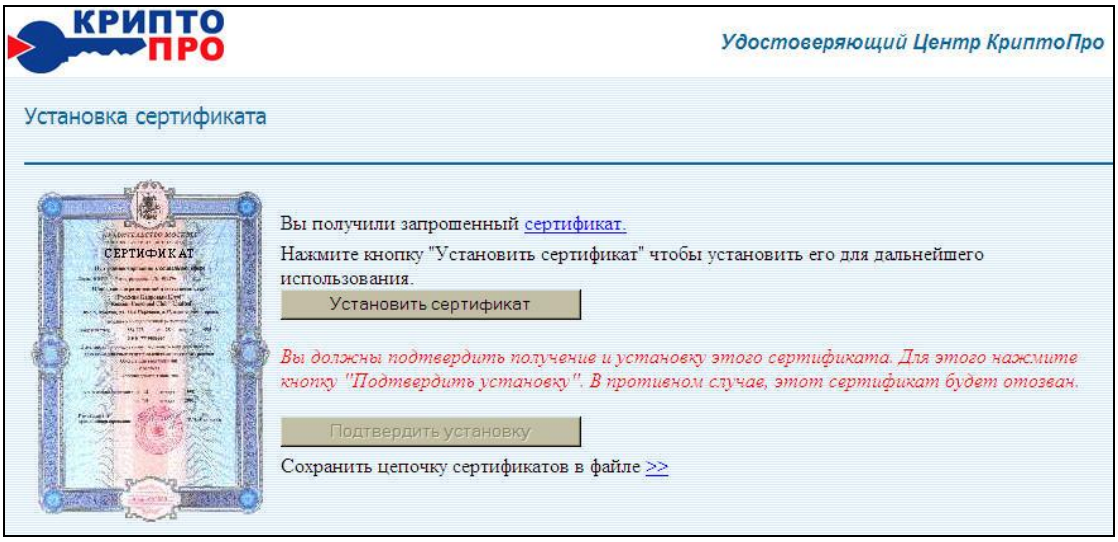


Рисунок 16 – Установка сертификата

Приложение 1

Правила заполнения поля «Общее имя»

В качестве исходных данных для значения поля используются фамилия, имя и отчество. Необходимо провести транслитерацию этих данных согласно с приведённой ниже таблицей.

Таблица 1. Правила транслитерации

Рус.	**Англ.**		**Рус.**	**Англ.**		**Рус.**	**Англ.**
а	a		х	h		М	M
б	b		ц	c		Н	N
в	v		ч	ch		О	O
г	g		ш	sh		П	P
д	d		щ	sch		Р	R
е	e		ы	y		С	S
ж	zh		э	e		Т	T
з	z		ю	yu		У	U
и	i		я	ya		Ф	F
й	y		А	A		Х	H
к	k		Б	B		Ц	C
л	l		В	V		Ч	Ch
м	m		Г	G		Ш	Sh
н	n		Д	D		Щ	Sch
о	o		Е	E		Ы	Y
п	p		Ж	Zh		Э	E
р	r		З	Z		Ю	Yu
с	s		И	I		Я	Ya
т	t		Й	Y			
у	u		К	K			
ф	f		Л	L			

Вместо буквы «Ё» следует использовать букву «Е» и соответствующее правило транслитерации. Все остальные буквы и символы необходимо исключить. Далее, необходимо сложить получившиеся фамилию и первые буквы имени и отчества в одно слово. Это и будет значение для поля «**Общее имя**».

Например, «**Иванов Петр Михайлович**» транслитируется в «**Ivanov Petr Mihaylovich**», общее имя получается «**IvanovPM**».

Инструкция по форматированию Rutoken

Данная инструкция предусмотрена для драйвера Rutoken версии не ниже 2.57.

Необходимая последовательность действий:

1. Вставить носитель типа Rutoken в USB-порт компьютера; убедиться, что он горит ровным светом;
2. Открыть «Панель управления» (*Пуск – Панель управления*);
3. Выбрать пункт «Панель управления Рутокен»;
4. На вкладке «Администрирование» в пункте «Считыватель Rutoken» выбрать вставленный носитель;
5. Нажать кнопку «Login…» и авторизоваться на ключе в качестве Администратора (пароль по умолчанию *87654321*);
6. В пункте «Форматирование токена» нажать кнопку «Форматировать…»;
7. Настройки форматирования определяются пользователем, однако обязательно должны быть выполнены следующие пункты:
    a. Снять флаг «Использовать PIN-код по умолчанию» в пункте «Пользователь»;
    b. Ввести «Новый PIN-код» и его «Подтверждение»;
    c. Выставить переключатель «Политика смены PIN-кода Пользователя» в положение «Администратором».
8. Дождаться окончания форматирования и закрыть «Панель управления Рутокен».

Носитель готов к записи ключа.

Инструкция по форматированию eToken

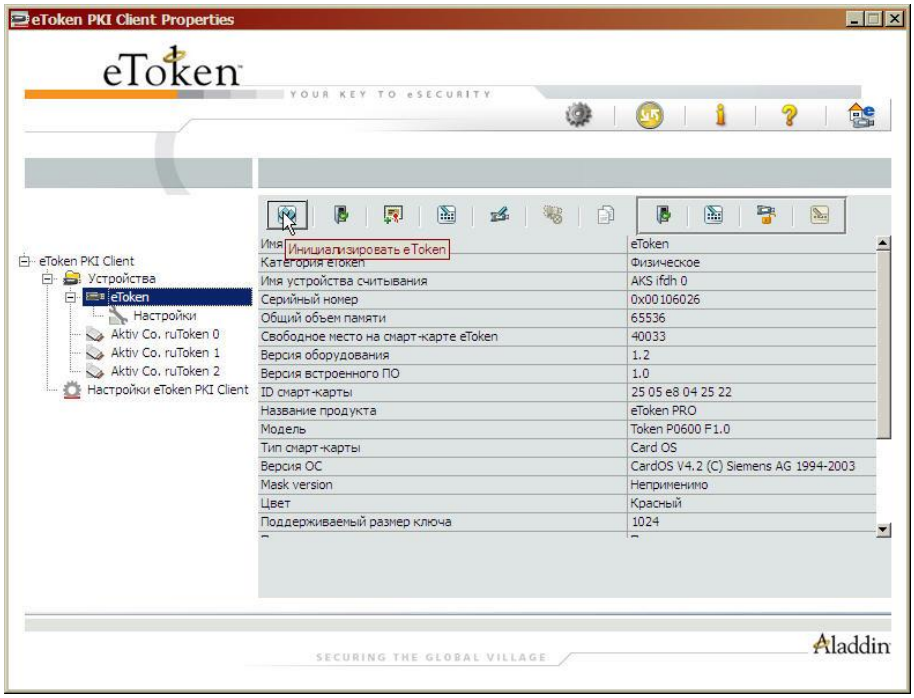
Данная инструкция предусмотрена для драйвера eToken PKI Client версии не ниже 5.1 SP1.

Необходимая последовательность действий:

1. Вставить носитель типа eToken в USB-порт компьютера; убедиться, что он горит ровным светом;
2. Открыть «eToken PKI Client Properties» (*Пуск – Все программы – eToken – eToken PKI Client – eToken Properties*);
3. Нажать на пиктограмму шестерёнки, чтобы перейти к режиму отображения «Подобный вид»;



4. В дереве выбрать необходимое устройство и нажать на кнопку «Инициализировать eToken»;



5. Настройки форматирования определяются пользователем, однако обязательно должны быть выполнены следующие пункты:
    a. Поставить флаг «Пароль пользователя» и ввести его и «Подтверждение»;
    b. Снять флаг «При первом входе необходимо изменить пароль».
6. Дождаться окончания форматирования и закрыть «eToken PKI Client Properties».

Носитель готов к записи ключа.

Приложение 3

Порядок предоставления сертификатов УЦ Минздравсоцразвития России посредством веб-доступа

Для получения сертификата УЦ Минздравсоцразвития России посредством веб-доступа необходимо:

1. Отправить заверенную руководителем учреждения заявку на выпуск сертификата (форма заявки расположена на сайте УЦ по адресу http://crt.rosminzdrav.ru/F1.doc) официальным письмом на адрес Департамента информатизации;
2. Подготовить рабочее место в соответствии с требованиями, описанными Пункте 2 Руководства;
3. При наличии сертификата пользователя, полученного в УЦ Минздравсоцразвития России, выполнить «Вход зарегистрированного пользователя» (Пункт 5 Руководства), в ином случае подать запрос на регистрацию, получить маркер временного доступа и выполнить последующие действия для получения сертификата пользователя (Пункты 3, 4 Руководства). Если сертификат пользователя имеется, но срок его действия уже истёк, необходимо обратиться в Департамент информатизации с просьбой предоставить маркер временного доступа, указав данные пользователя, использованные при регистрации (дальнейшая работа с маркером соответствует описанной в пункте 4 Руководства).

Внимание! *Выпуск сертификата возможен только в случае наличия оригинала Заявки на выпуск сертификата в УЦ Минздравсоцразвития России*.

Примечание: *Криптопровайдер для работы с электронными ключами доступа в системе доступен по адресу http://download.gasurf.ru/crypto_x86_v2.0_tr.zip (для 64-битной версии ОС - http://download.gasurf.ru/crypto_x64_v2.0_tr.zip)*

Примечание: *Выпуск сертификатов непосредственно на территории УЦ возможен только в случае наличия оригинала Заявки на выпуск сертификата в УЦ Минздравсоцразвития России. Получить сертификат может владелец сертификата лично или его доверенное лицо, при наличии Доверенности на получение сертификата (Форма доверенности на сайте http://crt.rosminzdrav.ru/Dov.doc)*